

Issues and challenges of regulation of relations on the Internet to guarantee adherence to human rights

by Svitlana M. Zadorozhna*, Irina V. Aristova[^], Iryna Yu. Tatulych[°],
Pavlo S. Ivanitskyi[§], Olha I. Khodoba**

Abstract

This article addresses the critical issue of human rights protection in digital environment, with the legal frameworks governing digital rights as a core concept. The main research questions examine key threats to human rights online and effectiveness of existing international and national mechanisms for safeguarding these rights. The study employs a comparative analysis of legal systems and their modifications responding to the impact of evolving digital technologies and markets in the EU and the U.S. The study also addresses how Internet access has impacted user rights during the Russian-Ukrainian war. Using formal-legal and systemic methods, the research assesses the effectiveness of these regulatory approaches. The results reveal significant differences in protection of digital rights across the EU, the U.S., and Ukraine, highlighting gaps in enforcement and practical application. The findings contribute to the ongoing discourse on the need for stronger global collaboration in digital rights regulation and propose recommendations for

* Doctor of Law, Professor Department of International Law, Faculty of Law, Yuriy Fedkovych Chernivtsi National University, 58012, 2 Kotsiubynskyi Str., Chernivtsi, Ukraine, e-mail: s.zadorozhna@chnu.edu.ua, ORCID: 0000-0003-2681-7855.

[^] Doctor of Law, Professor Department of Administrative and Information Law, Sumy National Agrarian University, 40000, 160 Herasym Kondratiev Str., Sumy, Ukraine, ORCID: 0000-0001-9211-3464.

[°] PhD in Law, Associate Professor Department of Procedural Law, Faculty of Law, Yuriy Fedkovych Chernivtsi National University, 58012, 2 Kotsiubynskyi Str., Chernivtsi, Ukraine, ORCID: 0000-0003-0482-8174.

[§] PhD Student Department of Theory of Law and Human Rights, Faculty of Law, Yuriy Fedkovych Chernivtsi National University, 58012, 2 Kotsiubynskyi Str., Chernivtsi, Ukraine, ORCID: 0009-0003-8944-4424.

** Master of Law, Assistant Department of International Law, Faculty of Law, Yuriy Fedkovych Chernivtsi National University, 58012, 2 Kotsiubynskyi Str., Chernivtsi, Ukraine. Department of Social Protection, Chernivtsi Regional State Administration, 58002, 1 Hrushevskyi Str., Chernivtsi, Ukraine, ORCID: 0000-0002-8457-8883.

Rivista di Studi sulla Sostenibilità - Open access (ISSNe 2239-7221), 2025, 2

Doi: 10.3280/riss2025oa19632

enhancing legal protections in the digital sphere, particularly in Ukraine's context. This research advances the understanding of how international legal standards can be integrated into national legislation, offering new perspectives for policymakers and legal scholars.

Keywords: Internet, human rights and freedoms, information rights, digital freedom, international law.

First submission: 7 March 2025; *accepted:* 14 July 2025

Introduction

In the modern digital age, human rights issues have acquired new meanings since governments are required to develop legislative mechanisms to protect and maintain fundamental rights in the digital space. In this regard, legal support should empower both businesses and individuals, ensure and guarantee rights and freedoms enshrined in the European Convention on Human Rights, which are implemented in the digital sphere (Aristova et al., 2021). Human rights are fundamental to democratic societies and reflect the principal values and principles that ensure freedom, security, and dignity of every person (Holovko et al., 2021). In the EU countries, the U.S., and Ukraine, human rights are given great importance; they are documented in detail in national and international documents. The EU and the U.S. are among the most significant regions in terms of digital technology development, policy adoption, and global influence. Regulations often set trends affecting other jurisdictions worldwide. Hence, the analysis of the EU and U.S. legislation on Internet provides insight into global standards and practices in the field of digital rights. In the EU, they are enshrined in the Charter of Fundamental Rights of the European Union and the European Convention on Human Rights, in the U.S. digital rights are defined in the Constitution and the Bill of Rights, while in Ukraine, they are provided for in the Constitution and laws governing the rights and freedoms of citizens. These documents enshrine the values that form the foundation for the rule of law, including equality, freedom, privacy, non-discrimination, human dignity, inclusiveness, and democracy. These values include freedom of expression, the right to privacy, protection from discrimination, and the right to redress in cases of rights violations.

Basic rights such as privacy, freedom of expression, and personal sovereignty are greatly affected by the rise of digital technology. The impact of digitalization is observed in all spheres of life, which brings both opportunities and threats to the realization and protection of these rights. The state and private companies, possessing large amounts of personal data, are

able to violate the privacy of citizens and have the ability to control digital platforms, which jeopardizes freedom of speech. During warfare, when the online space becomes a field for information wars and a tool for mobilizing the population, these risks become even more acute. In other words, the Internet has become a means of manipulating public opinion and a platform for violating people's rights to privacy and freedom of expression, in particular through the use of technology for surveillance and control.

In the context of digital transformation, the question arises whether digitalization creates new rights for users? This right can be interpreted as the right to privacy and autonomy in the digital environment. This is especially acute in the face of the constant growth of digitalization and the introduction of new technologies that provide access to vast amounts of information and create new challenges for personal privacy. In traditional legal framework, the right to privacy provided for the protection of privacy and information from interference by the state or third parties. However, in the context of digitalization, this right takes new forms. For example, the right to freedom from intrusive advertising, the right to protection from cyberbullying, and the right to be forgotten require that a person can control what data about him/her is available on the Internet. In such a way, a person can defend his/her personal integrity in the digital space. These issues prompt discussions about the need for new legal mechanisms that can adequately protect the rights of users on the Internet.

Therefore, the aim of the article is to establish the main problems and challenges in regulations of relations on the Internet, related to the observance of human rights, and analyze the approaches of different countries to address these issues on the example of the EU, the U.S, and Ukraine. Accordingly, the hypothesis that the effectiveness of legal protection of human rights in the digital environment depends on the integration of international standards, national regulatory mechanisms, and clear state enforcement. Therefore, the novelty of the article consists in filling the gaps in the study of practical aspects of law enforcement and the integration of international norms into national legislation. This research also suggests new approaches to the analysis of digital rights protection not only by legislative acts, but also through mechanisms of international cooperation and legal standards harmonization in the global digital space.

In order to achieve the aim of the research, a number of research methods is applied. Thus, the analysis of the regulatory framework is carried out, including the study of international acts such as the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, the EU General Data Protection Regulation (hereinafter – GDPR), and the U.S. California Consumer Privacy Act (2018) (hereinafter – CCPA). This analysis

helps understand the basic principles of legal protection in the digital sphere. This stage facilitates assessing differences in approaches to the digital rights regulation, using legal frameworks such as GDPR and CCPA as key examples. In particular, the principles on the protection of privacy, freedom of speech, and cybersecurity are investigated. Moreover, the mechanisms of control and practices of Internet companies in EU, the U.S, and Ukraine are compared.

Furthermore, the content analysis is used to analyze case law on digital rights violations, in particular in cases of blocking content or illegal data collection. In addition, the academic literature is analyzed to identify key challenges and approaches that affect human rights on the Internet. The quantitative and qualitative analysis of statistical data on citizens' complaints about violations of rights on the Internet in Ukraine, the EU and the U.S. is also carried out. This statistical analysis helps assess the effectiveness of existing legal mechanisms of protection. Moreover, the method of comparative legal analysis allows the researchers to identify gaps in regulations and determine directions for improving the digital rights regulation. In this regard, the results of the implementation of different legal norms and their impact on freedom of speech and privacy in different countries are compared.

The system method is used to determine the relationships between different legal institutions and mechanisms that protect human rights in the digital space. This approach made it possible to consider regulation as an integral system functioning in the interaction of international and national law. This multidimensional approach ensures research reproducibility and facilitates the evaluation of the reliability and validity of results.

Discussions on the protection of human rights in the digital environment: Literature review

The problem of human rights on the Internet has always been relevant in modern Ukrainian legal doctrine. Currently, the basic doctrinal provisions on human rights in the digital space have not been significantly changed. It should be noted that all theoretical developments regarding human rights on the Internet are mainly based on the proclamation of guaranteeing any human rights in the digital space as a modern way of their implementation (Holovko et al., 2021). In this regard, each right or freedom on the Internet is investigated as a specific opportunity.

When studying the guarantees of human rights in the digital environment, considerable attention is paid to the analysis of the main approaches to their

regulation in various jurisdictions. A review of academic sources shows that most authors focus on privacy and data protection issues, as well as the need to strengthen regulatory mechanisms to prevent rights violations online (Sarakutsa & Piliuk, 2021).

According to Bocharova (2021), the information society is developing in a new paradigm, where information and knowledge become the main products of human activity. Moreover, technologies perform not only a technical function, but also serve as a social tool for realizing human potential. However, the widespread use of technology can adversely affect fundamental human rights, especially in the face of insufficient privacy protections and a lack of clear regulations of digital platforms. The Internet can also have a detrimental effect on democracy and human rights through the use of algorithmic filters that provide users with information that matches their beliefs. As Rosmetaeva (2020) claims, this can strengthen prejudice and cause radicalization of views, which in turn affects the tolerance level in society.

Furthermore, Mironyuk (2021) focuses on the need to create state mechanisms for the implementation of human rights on the Internet and increase the legal awareness of citizens regarding their rights and obligations in the digital space. Although most studies emphasize existing legislative initiatives, issues related to practical enforcement and the interaction between international and national norms remain understudied.

The comparison of different approaches to human rights protection on the Internet on the example of the GDPR (European Parliament and Council of the European Union, 2016) in the European Union and the CCPA (2018) in the United States highlights the differences in the protection of users' rights in these regions. However, they do not focus on the digital environment impact on human rights in crisis situations. The EU is known for its proactive and comprehensive approach to the digital environment regulation through the GDPR, which focuses on privacy and user consent. In turn, the U.S. has a more fragmented regulatory landscape that often favors innovation and economic growth over strict privacy protections. This distinction facilitates a rich comparative analysis of how different philosophical frameworks can shape digital rights and freedoms. While the EU regulations may provide stronger privacy protections, the U.S. system may facilitate faster technological innovation. Understanding these complementary perspectives can inform policy makers and stakeholders about potential lessons and best practices.

At the same time, both the EU and the U.S. face similar challenges arising from rapid technological progress such as cybersecurity issues, disinformation, and the ethical aspects of AI. The literature review shows

that human rights on the Internet are under threat due to a number of factors such as privacy violations, restrictions on freedom of speech, and the influence of algorithms on the formation of public opinion. Modern literature offers different approaches to solving these problems although the development of universal standards and mechanisms is necessary to ensure the protection of human rights on the Internet, regardless of the jurisdiction and specifics of a particular country. In addition, there is a lack of comprehensive analysis of how countries with different cultural and legal traditions can integrate international standards of digital rights into their legal systems.

Statistics on citizens' complaints about violations of human rights in the digital space

The realities of the modern stage of development of civilization and society give rise to new forms of activity and relations between people who naturally use all the privileges of information and technological development of society. The information society today is seen as a new historical phase of civilization, in which the main products of human activity are information and knowledge, and technology is becoming important not only technical means but also social tools for realizing human potential. The information model of building the future society has become a new paradigm of social development as opposed to the past mechanistic paradigm (Bocharova, 2021).

This model of building a social order allows people to fully unleash the full potential of technology, such as the Internet, which creates new responsibilities both in the societies of individual states and in the world as a whole. Using technology can be as much a problem-solver as a problem-creator. Such tools have the potential to advance justice and equality, bolster the foundations of democratic governance, and guarantee transparency, accountability, and engagement between the public authorities, individuals, and groups. It is evident that one of the most significant developments of the information era is the Internet. Its unprecedented proliferation and influence warrant particular attention and recognition (Razmietaieva, 2020). This, in turn, raises a range of various challenges related to the regulation of human rights issues that need to be put on the agenda in all civilized countries seeking to ensure respect for human rights, at all levels, including both international and national.

Today, according to Worldometers (2024), 7.8 billion people live on our planet. According to the UN, 4.2 of them use the Internet. At the beginning

of 2020, the number of new Internet users increased by 298 million compared to January 2019, i.e. by 7%. However, the coronavirus epidemic, which began in early 2020, changed the life of the planet, demonstrating the extreme importance of the Internet for modern man. This is evidenced by recently published UN statistics: in a pandemic, Internet traffic has tripled. These changes have affected the world, and at the same time the so-called digital divide has become even more apparent. After all, 3.6 billion people worldwide lack access to the Internet (Novytskyi, 2016).

The statistics indicate numerous complaints of citizens regarding violations of rights in the digital sphere. For example, during the COVID-19 pandemic and the war in Ukraine, the number of cases where online platforms are used to spread misinformation or promote hatred has increased, making it difficult to monitor and respond to such violations. According to the data, the rights of Internet users, who are victims of violations, are poorly protected in Ukraine. This fact emphasizes the need to improve the legal framework and introduce effective mechanisms for restoring violated rights.

In the 21st century, the issue of human rights protection in the Internet is very important because the development of technology, the achievement of scientific and technological progress require legal regulation. Cyber security provides protection of resources, information, data at the stage of their exchange and storage. After all, not everyone understands their rights and responsibilities in the space of the latest technologies (Myroniuk & Halak, 2021).

Modern people, even if they have information about their rights and responsibilities, do not often understand how to protect or restore violated rights, and the issue of these rights in the context of the Internet further deepens the misunderstanding and inability of people to protect and restore their rights. It is a question of creation of the state mechanisms of realization of these rights, and their normative fixing. In the digital sphere, human rights and freedoms are violated in various ways. On the one hand, governments can commit the most egregious violations such as mass surveillance, censorship of the Internet content, arrests of journalists and activists for their online activities. For example, in countries with authoritarian regimes (Belarus or China), governments control access to information and block social networks to suppress opposition. On the other hand, individuals can also violate the rights of others in the digital environment by cyberbullying, disclosing personal information without consent (the so-called “doxing”) or slandering. Every modern person should know how to protect their rights on the Internet, how not to become a victim, how to prevent the negative consequences of violations of subjective rights and where to go to restore the violated rights (Myroniuk & Halak, 2021).

At present, statistical data on civil and administrative complaints lodged by citizens concerning infringements of human rights and freedoms in the digital domain indicate that the safeguarding of the rights of Internet users who have been subjected to violations remains severely constrained in Ukraine. This situation calls for the reinforcement of legal frameworks and the implementation of effective mechanisms for the restoration of violated human rights, particularly in instances where the Internet has been the conduit for such infringements (Kurtakova & Usmanov, 2020).

The rights that individuals have offline (e.g., freedom of speech, privacy) are the same as those they have online. However, the way these rights are exercised or how responsibilities are fulfilled can differ between the two settings. The main distinction is not in the rights themselves but in how they are practiced or enforced. For instance, privacy in the offline world might involve physical privacy, whereas online it involves digital data protection. Just like in the offline world, activities conducted online can lead to human rights violations (e.g., online harassment, illegal surveillance). Individuals and entities can be held accountable for these violations, reinforcing that human rights standards apply in both settings.

Some scholars believe that rights in offline mode cannot be compared with rights on the Internet. Thus, Sardak et al. (2021) note that the digital environment creates new challenges that can exacerbate the issue of freedom of speech and privacy. They emphasize that anonymity on the Internet can lead to impunity in cases of slander or threats, which jeopardizes users' responsibility for their actions. Studies conducted by the UN confirm that anonymity on the Internet can interfere with the effective protection of individual rights since sometimes anonymous accounts hide persons who commit crimes in cyberspace.

Hence, the rights that people have offline (for example, freedom of speech, privacy) remain the same in the digital sphere. Nevertheless, the ways of their implementation and responsibility for their violation may differ significantly. In this regard, it is important to ensure proper mechanisms for the realization of users' rights on the Internet and their restoration in case of violation.

The need for regulating relations online

In this regard, a number of new threats are emerging that have not been on the agenda of world organizations, state institutions and civil society until recently. The modern world, like Ukraine, with the technological progress has entered the era of information threats, cyberattacks and, accordingly,

information wars. Individual information wars can be much more effective than conventional ground wars with the use of people, territory and weapons, as they affect indefinite areas through the use of information capabilities (Sopilko, 2017). An obvious and horrific example of this is the Russian-Ukrainian war, which clearly shows what information warfare is and how the use of Internet technology for military or criminal purposes can have serious consequences for the information society and access to truthful and verified information from official sources, cyberattacks and other information threats.

With the development and spread of the Internet, more and more countries around the world are aware of the need for its legal regulation. Primarily, this can be attributed to the Internet's significant impact on societal evolution, particularly in regard to its role in facilitating revolutionary changes across all aspects of life. The Internet is a significant factor in social, economic, and cultural development that presents new possibilities for public authorities and ordinary citizens and educators. It has facilitated the creation and dissemination of materials, removed barriers to access, and provided universal access to an expanding array of digital sources (Kovalenko & Turov, 2017). This proves that the range of Internet sources does not mean the criteria of quality or truthfulness, which again opens the problem of regulation of the activities of people and government agencies or institutions on the Internet.

The regulation of the Internet is an issue of significant importance, particularly in view of the necessity to consider the information and communication network as a vehicle for the realization of almost any human right. In any situation wherein rights are acknowledged, responsibilities must also be recognized. It is always possible for these responsibilities to be violated. Consequently, the feasibility of exercising rights and freedoms through digital platforms, along with the prevalence of infringements upon these rights and freedoms, substantiates the imperative for the enactment of diverse levels of legal instruments. Nevertheless, the Internet self-regulating community cannot create a free information environment or set clear rules for Internet users. In particular, the non-binding and non-universal nature of recommendations and resolutions, among other acts, limits the effectiveness of this approach in guaranteeing the aforementioned freedoms.

It has recently become increasingly clear that the regulation of Internet governance requires the adoption of acts that contain international legal norms which bind national legislatures. The framework of international Internet law has developed, with the objective of regulating a series of key issues pertaining to the governance of the Internet. These include relations between states in the digital space, the implementation of controlling

measures, and the respect for citizens' rights in this digital age (Sarakutsa & Piliuk, 2021). At the present stage of international cooperation, it is not difficult to develop a universal act to guarantee respect for human rights in the network, it is simplified by the presence of alliances and the number of international agreements with dozens of participating countries.

It should be emphasized that scientists in Western Europe have been analyzing the legal aspects of the Internet information environment for many years. Numerous reports and reports on electronic networks, law and the Internet, prepared at the request of public authorities, have been published in full in France, Belgium, Germany, the U.S. and the UK. Such work is carried out constantly. Its purpose is to study the dynamics of functioning, the development of the Internet as a new way of communication in the world and to develop means of legal and ethical influence on people.

Such analytical work, involving a wide range of scientists and legal experts, should also be conducted regularly in Ukraine and the CIS countries. And this is inevitable, because our market as an integral part of the global market for goods and services is already facing an urgent need for Internet services and is experiencing significant losses due to the lack of scientifically sound and flexible legal regulation of relations arising on the Internet. Thus, creating the concept of information development of Ukraine is critical. There are clearly not enough conceptual acts in this field of informatics and technologies, and there are no special documents dedicated to the Internet at all (Lytvynov, 2013).

Even the simplest, such as defining the legal status and significance of the Internet, is not present in modern domestic acts, let alone a universal act, perhaps even an international one, to be ratified by the Verkhovna Rada of Ukraine. However, these legal documents cannot comprehensively cover the full breadth of online relationships, as well as provide all the prerequisites for protecting and fulfilling human rights online. This once again shows the importance and urgency of establishing mechanisms and adopting regulations, in particular laws and international treaties, that will address the issue of the Internet regulation or will directly regulate these relations.

In the development of modern legislation, we must proceed from the fact that the Internet is a public environment, a public space, and it is used for economic activities and for gathering information. The Internet is changing our space, making it virtual. But in this virtual space, not virtual laws should apply, but the same regulations that govern ordinary space. In light of the ongoing transition toward a more information-centric society, it is necessary to legally enshrine its basic elements (Hlukha, 2020). The components of the Internet correspond to ordinary life, such as the cultural, economic or social

spheres, which are directly regulated by legislation, to which must be added the regulation of these rights online.

The Internet is the basis for the development and consolidation of the main directions. Any interference by the state in the network is perceived by the Internet community as a violation of its rights, because currently regulation is through public scrutiny. In order to regulate the network, it is necessary to analyze the trends that are emerging in the online community, consolidating the aspects that it has recognized (Lytvynov, 2013). That is, it is necessary to take into account the opinion of network users, and in general to be guided by the usual principles according to which the Internet operates despite the lack of legal status or regulation.

There is no single special body within the European Union to regulate the Internet. In 2004, the European Network and Information Security Agency (ENISA) was created to act as a consultant and center of advanced technologies in the field of network and information security for the EU member states and institutions. In January 2013, the European Cybercrime Center was established, whose task is to stop the activities of organized criminal networks. The Council of Europe Convention on Cybercrime (2001), the Privacy and Telecommunications Directive (2002), the Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive) (2016) aim to establish common cybersecurity standards and improve cooperation between EU countries, are in force in the EU (European Parliament, 2016). Although there are documents that directly regulate human rights that can be applied to online relations, most of them apply to international acts that are recognized by most countries in the world, or their region, if it is a regional act (Hutsu, 2018).

The key international instruments guaranteeing human rights and freedoms are the Universal Declaration of Human Rights (1948), the International Covenant on Civil and Political Rights (1966), the International Covenant on Economic, Social and Cultural Rights (1966), the Convention for the Protection of Fundamental Rights and Fundamental Freedoms (1950), the Charter of Fundamental Rights of the European Union (2000), and the Convention on the Rights of the Child (1989). The objective of this initiative is to advance the concept of respecting and safeguarding human rights online. Moreover, it should help international organizations develop and implement a number of recommendations, conventions, guidelines, etc. Documents produced by the United Nations, the United Nations Children's Fund (UNICEF), the Council of Europe, the European Union, and other international organizations focus on the adherence to human rights with the digital setting. States are changing national legislation to realize human rights in the digital space (Voitsikhovskiy, 2018).

The notion of digital rights: challenges and threats

It can be said that the principal task for the observance of human rights and their protection relies on states, which must take international initiatives to legally establish the status of the Internet, enshrine acts in national legislation and cover uniform acts. Thus, the state not only has the rights but also the responsibilities to regulate these areas. This suggests that it is both within the state's power and its obligation to create laws and enforce regulations that govern public communication, including online content. However, there are certain circumstances where the state's regulation might conflict with or infringe upon human rights and freedoms. In other words, the state must do so in a manner that respects and does not unjustly violate fundamental rights and freedoms of its citizens.

State regulation is a definition of clear rules and control over their observance. In this sense and interpretation without regulation it is impossible to do in the field of national use of the Internet as a global information network. If these principles are established taking into account the positive world experience, focusing on democratic principles, then the more detailed and clear these principles will be developed and written, the more transparent will be the processes related to the use of the Internet (Omelchenko, 2014).

At the same time, the Internet can have a detrimental effect on democracy and human rights. This is consistent with the statement that rights are the same online and offline as it emphasizes the importance of the context of their implementation. While rights remain the same, the way they are exercised and protected in the online environment can be more complex due to the specificity of digital technologies. For example, content filtering algorithms used in social networks can create information bubbles in which users receive information confirming their views. This can deepen polarization, radicalize thoughts, and decrease social tolerance (Razmietaieva, 2020).

Thus, the rights that people have online may be at greater risk due to factors such as misinformation, cyberbullying, censorship, and insufficient privacy protections. These risks can undermine the foundations of democracy because they prevent the formation of an objective and diverse information base necessary for an informed civil society. In the face of such a threat, the state protection of human rights in the digital sphere should be strengthened. This may include the development of legislation that regulates issues of privacy and data security, as well as mechanisms that allow the government to effectively respond to rights violations in the digital environment.

Furthermore, in order to ensure rights and freedoms in the digital sphere, it is important to find a balance between protecting these rights and ensuring freedom of speech. In other words, the rules for using the Internet should be aimed at protecting users from abuse, while not restricting their rights to free expression. In this context, it is important to take into account not only the duties of the state to protect the rights of citizens, but also the need to inform society about their rights and ways to protect them in a digital environment.

It is necessary to realize that freedom in the Internet space is one of the most important elements in the creation of acts designed to regulate relations and the exercise of rights in the network. What about digital rights? Analyzing the scientific literature, it is possible to claim that the digital rights encompass several fundamental entitlements, including the freedom and personal security of individuals within the online domain; the right to privacy; the freedom of expression in the digital sphere; the right to peaceful assembly and association; the utilization of digital instruments of democracy; and the prerogative of digital self-determination, or the capacity to disengage from the digital space.

As can be seen from the above, the content of digital rights does not differ significantly from the category of fundamental human rights, except for one – they are all carried out on the Internet, or through its use. It seems quite logical to understand digital rights as a mode of realization of fundamental human rights. From the standpoint of dialectics, basic human rights and digital rights are correlated as content and form (Marushchak, 2021). Therefore, despite the existence of acts regulating fundamental human rights, an important aspect now is the regulation of these same rights online.

The online environment is actively entering the life of the average citizen, through the use of social networks, online platforms, electronic, which indicates that we live in the period of the fourth industrial revolution. However, it has posed a scope of challenges that need to be dealt with immediately, taking into account the core standards of the Council of Europe and the ECtHR case law. The objective is to establish an online environment that safeguards ownership, privacy, and personal data in accordance with the standards of freedom of expression, both in physical and virtual spaces (Sopilko, 2017). Therefore, the importance of the Internet regulation to ensure human rights is immense. The creation of international and national legislation presents a challenge that the world must address comprehensively to uphold human rights against current and future threats.

Digital rights protection in the EU, U.S., and Ukraine

To deepen the analysis of digital human rights, it is essential to explore

how different countries regulate these rights and deal with the emerging problematic aspects of the digital era. For instance, a comparison of the GDPR and the CCPA highlights significant differences in legal frameworks. While the GDPR provides a comprehensive, centralized approach to ensuring individuals' privacy rights, the CCPA offers a more fragmented, state-level regulatory mechanism. The GDPR is known for its stringent requirements, such as obtaining explicit consent before processing personal information and ensuring the right to be forgotten, thus empowering European citizens to control their digital presence. In contrast, the CCPA affords California residents the right to be informed as to the nature of the data being collected and the option to decline participation in data sales. However, it lacks the broader enforcement mechanisms found in the GDPR.

Moreover, the enforcement of these regulations differs significantly. The GDPR has the power to impose heavy fines on companies that fail to comply. The potential penalties for noncompliance can reach up to four percent of a company's global annual revenue. This has led to a higher level of compliance and awareness among European businesses about data privacy. Meanwhile, the CCPA's penalties are more limited, and enforcement primarily depends on the actions of the Attorney General of California, leading to uneven enforcement and compliance across different sectors. These contrasts illustrate not only the diversity in legal approaches but also the varying degrees of protection provided to individuals' rights online, depending on the jurisdiction in which they reside (European Parliament and the Council of the European Union, 2016).

In addition, a study on the role of Internet during the pandemic underscores the global need for stronger digital rights protections. In countries like South Korea, where technology was effectively used to trace and control the spread of the virus, the balance between public health measures and privacy rights became a focal point of legal debates. Meanwhile, in Ukraine, the use of social media platforms during the Russian-Ukrainian war to document human rights violations has prompted discussions about the need for international legal standards that ensure the right to free expression online while mitigating the risks of disinformation and privacy breaches.

The synthesis of these comparative perspectives and case studies reinforces the argument that legal frameworks must evolve to address both the opportunities and threats posed by the digital space. The effective regulation of digital rights is not only a national issue but a global one, requiring coordinated international efforts (Bocharova, 2021; Razmietaieva, 2020). By bridging the gap between theoretical approaches and practical case

studies, it becomes evident that the upholding human rights on the Internet requires a comprehensive, multilayered legal response.

Conclusions

Since today the information and communication sphere and the Internet are a means of realizing almost any human rights and freedoms, the range of violations of these rights and freedoms is increasing as the digital age of mankind develops. Therefore, thanks to legal regulation, the Internet should not become a sphere of breach of human rights and freedoms, but a sphere of cross-border guaranteed, safe and free space for the development of the person.

The importance of the Internet for the military situation in Ukraine cannot be overestimated, as it is an opportunity to disseminate and transmit important, strategic and sometimes vital information, military strategy, fundraising and volunteering, collecting information and evidence of Russian war crimes in Ukraine, military medical training of the population, psychological support of victims and a number of other important aspects. inadequate legal regulation deprives human rights of protection and guarantee, so the improvement and evolution of digital legislation must always remain alive.

This study makes a significant contribution to the field of legal regulation of digital rights, in the context of upholding human rights on the Internet. The comparative analysis shows that regulatory approaches differ significantly, regarding privacy and personal data protection. The study also emphasizes the importance of international cooperation and harmonization of legal standards for more effective guarantees of human rights in the digital sphere. The example of Ukraine demonstrates the need to strengthen legal regulation in times of war, when the Internet is essential in protecting the rights of citizens.

However, the study has certain limitations. The main one is that it is based on secondary data and comparative analysis of legal acts, which does not take into account the details of their practical application in specific cases. In addition, the study is limited to a few jurisdictions, so further research could focus on analyzing regulatory approaches in other countries or regions to provide a more global picture.

Suggestions for future research include conducting empirical studies covering the practical aspects of the application of digital rights in different jurisdictions. It is also worth focusing on the role of international

organizations in shaping common standards for upholding human rights in digital environment.

References

- Aristova I., Brusakova O., Koshikov D., & Kaplya O. (2021). Developing Information Technology Law and Legislation: Analysis of International Experience and Possibilities of Its Application in Ukraine. *Ius Humani. Law Journal*, 10(2): 117-128. Doi: 10.31207/ih.v10i2.287.
- Bocharova N.V. (2021). Ensuring human rights in the information society: Problems of creating an international bill of human rights on the internet. In *The Latest Achievements and Vectors of Development of Modern Jurisprudence* (pp. 33-60). Kyiv: Liha-Pres. Doi: 10.36059/978-966-397-244-2-1-2.
- Buriachok V.L., Tolubko V.B., Khoroshko V.O., & Toliupa S.V. (2015). *Information and cyber security: social and technical aspect*. Kyiv: DUT.
- California Consumer Privacy Act (2018). -- Retrieved from <https://oag.ca.gov/privacy/ccpa>.
- Charter of Fundamental Rights of the European Union. (2000). Retrieved from https://www.europarl.europa.eu/charter/pdf/text_en.pdf
- Convention for the Protection of Fundamental Rights and Fundamental Freedoms (1950). -- Retrieved from https://www.echr.coe.int/documents/d/echr/convention_eng.
- Convention on the Rights of the Child (1989). -- Retrieved from <https://www.unicef.org/child-rights-convention/convention-text>.
- Council of Europe Convention on Cybercrime (2001). -- Retrieved from <https://rm.coe.int/1680081561>.
- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (2002). -- Retrieved from <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A32002L0058>.
- Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive) (2016). -- Retrieved from <https://digital-strategy.ec.europa.eu/en/policies/nis2-directive>.
- European Parliament and the Council of the European Union (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance). -- Retrieved from <https://eur-lex.europa.eu/eli/reg/2016/679/oj>.
- European Parliament (2016). Directive on security of network and information systems (NIS Directive). -- Retrieved from [https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/654198/EPRS_BRI\(2020\)654198_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/654198/EPRS_BRI(2020)654198_EN.pdf).

- Hlukha T. (2020). On the issue of features of legal regulation of relations in the Internet. In *IV International Student Scientific Conference "The Legal System of Ukraine in the Context of European Integration: The View of Student Youth"* (pp. 161-163) (Ternopil, May 2020). Ternopil: West Ukrainian National University. -- Retrieved from <http://confuf.wunu.edu.ua/index.php/confuf/article/view/149>.
- Holovko O.M., Aristova I.V., Shulhin V.V., & Sobakar A.O. (2021). Perspectives of electronic judicial proceedings' development: international experience and possibilities of its application in Ukraine. *Cuestiones Políticas*, 39(70): 66-79. Doi: 10.46398/cuestpol.3970.03.
- Hutsu S.F. (2018). Legal regulation of the internet: International and domestic experience. *National Technical University of Ukraine Journal. Political science. Sociology. Law*, 2(38): 114-118. Doi: 10.20535/2308-5053.2018.2(38).152935.
- International Covenant on Civil and Political Rights (1966). -- Retrieved from <https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights>.
- International Covenant on Economic, Social and Cultural Rights (1966). -- Retrieved from <https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-economic-social-and-cultural-rights>.
- Kovalenko L.P., & Turov V.D. (2017). On the problem of legal regulation of relations on the Internet. In *Internet of Things: Problems of Legal Regulation and Implementation: Materials of Scientific and Practical Conference* (pp. 233-237) (Kyiv, October 2017). Kyiv: National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute". -- Retrieved from https://ippi.org.ua/sites/default/files/zbirnik_2017__14.11.2017_-_vidredagovaniy.pdf.
- Kurtakova A.O., & Usmanov O.R. (2020). Protection of the rights of internet users as participants of private legal relations. *Scientific Perspectives*, 3(3): 91-99. Doi: 10.32689/2708-7530-2020-3(3)-91-99.
- Lytvynov Y. (2013). Legal aspects of the Internet functioning. *Legal Ukraine*, 10: 31-36.
- Marushchak A.V. (2021). Human rights in the era of digitalization. In N.V. Mishyna (Ed.), *Human rights in Ukraine and foreign countries: Traditions and novelties* (pp. 360-389). Lviv-Torun: Liha-Pres. Doi: 10.36059/978-966-397-235-0-13.
- Myroniuk O.I., & Halak A.V. (2021). Human rights protection in the Internet space. In *The XII International Science Conference "Topical tendencies of science and practice"* (pp. 208-210) (Edmonton, Canada, December 2021). Edmonton: International Science Group.
- Novytskyi A.M. (2016). Place of IT rights in the general system information law. In *IT Law: Problems and Prospects of Development in Ukraine: Collection of Materials of Scientific and Practical Conference* (pp. 116-119) (Lviv, November 2016). Lviv: Lviv Polytechnic National University.
- Omelchenko I.K. (2014). Ways to regulate internet content within the national legislation of Ukraine and international standards. *Information and Law*, 1(10): 73-86. -- Retrieved from <https://ippi.org.ua/sites/default/files/14oikums.pdf>.

- Razmietaieva Yu.S. (2020). Democracy, human rights and the Internet. *Law and Society*, 1: 104-110. Doi: 10.32842/2078-3736/2020.1-1.16.
- Sarakutsa M.O., & Piliuk S.V. (2021). International legal regulation of rights and freedoms on the Internet. *Analytical and Comparative Jurisprudence*, 3: 275-280. Doi: 10.24144/2788-6018.2021.03.51.
- Sardak S., Britchenko I., Vazov R., & Krupskyi O. P. (2021). Life cycle: Formation, structure, management. *Ikonomicheski Izsledvania*, 30(6): 126-142.
- Soldatenko O. (2018). Information space on the internet: Regulation and control. *Entrepreneurship, Economy and Law*, 5: 134-140. -- Retrieved from <http://pgp-journal.kiev.ua/archive/2018/5/27.pdf>.
- Sopilko I.M. (2017). Human rights and the internet: Features of their observance. In *VII International Scientific and Practical Conference "Human Security in the Context of Globalization: Modern Legal Paradigms"* (pp. 213-216) (Kyiv, February 2017). Kyiv: National Aviation University. -- Retrieved from <https://ocs.nau.edu.ua/index.php/strsp/7MNPk/schedConf/presentations>.
- Universal Declaration of Human Rights (1948). -- Retrieved from <https://www.ohchr.org/en/universal-declaration-of-human-rights>
- Voitsikhovskyi A.V. (2018). Protection of human rights and freedoms on the Internet. In *Protection of Human Rights: National and International Legal Dimensions: Materials of XIV International scientific Practical conference "From civil society – to the rule of law"* (pp. 543-549) (Kharkiv, May 2018). Kharkiv: V.N. Karazin Kharkiv National University.
- Worldometers. (2024). -- <https://www.worldometers.info/>.